

Status of the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Previously Presented) A method for providing an access candidate access to secured electronic data, the method comprising:

receiving a request for access candidate access to the secured electronic data by a controller associated with the secured electronic data;

comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the secured electronic data;

submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited; and

granting the access candidate access to the secured electronic data if the resolution authority provides authorization for such access.

2. (Previously Presented) The method as in Claim 1, further comprising granting the access candidate access to the secured electronic data in response to a comparison that indicates that access by the access candidate is not prohibited.

3. (Previously Presented) The method as in Claim 2, further comprising denying the access candidate access to the secured electronic data if the resolution authority denies authorization.

4. (Previously Presented) The method as in Claim 1, wherein the one or more access requirements associated with the secured electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to the controller via a network.

5. (Previously Presented) The method as in Claim 1, wherein the one or more access requirements associated with the secured electronic data are related to at least one of a citizenship status of the access candidate or a current location of the access candidate.

6. (Previously Presented) The method as in Claim 5, wherein the one or more attributes of the access candidate relates to the at least one of a citizenship status of the access candidate or a current location of the access candidate.

7. (Previously Presented) In a data security system having a first security level securing one or more resources for manipulating electronic data and a second security level securing access to the electronic data by the one or more resources, a method for providing an access candidate access to the electronic data, the method comprising:

- receiving a request for access to the first security level;

- granting the access candidate access to the first security level in response to a comparison of one or more attributes of the access candidate with one or more access requirements associated with the first security level that indicates that access to the first security level by the access candidate is not prohibited;

- receiving a request for access to the second security level;

- submitting a request for authorization to a resolution authority, which is configured to modify one or more access requirements associated with the second security level, in response to a comparison of one or more attributes of the access candidate with the one or more access requirements associated with the second security level that indicates that access to the second security level by the access candidate is prohibited; and

- granting the access candidate access to the second security level if the resolution authority provides authorization.

8. (Previously Presented) The method as in Claim 7, further comprising granting the access candidate access to the second security level in response to the comparison of the one or more attributes of the access candidate with the one or more access requirements associated with the second security level that indicates that access to the second security level by the access candidate is not prohibited.

9. (Previously Presented) The method as in Claim 7, further comprising denying the access candidate access to the second security level if the resolution authority denies authorization.

10. (Previously Presented) The method as in Claim 7, wherein the one or more attributes of the access candidate are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

11. (Previously Presented) The method as in Claim 7, wherein the one or more access requirements associated with the first security level relates to at least one of: a valid data access agreement with the access candidate; a current location of the access candidate; or, a citizenship status of the access candidate.

12. (Previously Presented) The method as in Claim 11, wherein the one or more attributes of the access candidate relates to at least one of: the existence of a data access agreement; a current location of the access candidate; or, a citizenship status of the access candidate.

13. (Previously Presented) The method as in Claim 7, wherein the one or more access requirements associated with the second security level relates to at least one of a current location of the access candidate or a citizenship status of the access candidate.

Reply to Office Action of January 4, 2010

14. (Previously Presented) The method as in Claim 7, wherein at least one of the request for access to the first security level or the request for access to the second security level is submitted by one or more sponsors.

15. (Previously Presented) In a data security system having a first security level securing one or more resources for manipulating electronic data and a second security level securing the electronic data, a method for providing an access candidate access to the electronic data, the method comprising:

identifying a plurality of data subsets of the electronic data;

determining, for each data subset, at least one data class associated with the data subset, the at least one data class identifying at least a citizenship requirement and a location requirement for access to data associated with the data class;

receiving, from a first sponsor of the access candidate, a request for access to the first security level, the request including an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate;

granting the access candidate access to the first security level based at least in part on an evaluation of the request for access to the first level;

receiving, from a second sponsor of the access candidate, a request for access to at least one data subset at the second security level in response to an indication that access to the first security level has been granted, the request for access to the at least one data subset including an indication of a citizenship status of the access candidate and an indication of a current location of the access candidate;

submitting a request for authorization to a resolution authority, which is configured to modify access requirements associated with the at least one data class, in response to a comparison of the citizenship status and the current location of the access candidate with the respective citizenship requirement and location requirement of the at least one data class of the requested data subset that indicates that access to a requested data subset at the second level by the access candidate is prohibited; and

Reply to Office Action of January 4, 2010

granting the access candidate access to the requested at least one data subset at the second security level if the resolution authority provides authorization upon receipt of the request for authorization.

16. (Previously Presented) A system for providing an access candidate access to secured electronic data, the system comprising:

storage configured to receive and store the electronic data;

one or more resources configured to access and manipulate the electronic data;

means for evaluating a request for access candidate access to the one or more resources, wherein the evaluation of the request includes a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the one or more resources;

means for granting the access candidate access to the one or more resources if the first comparison indicates that access is not prohibited;

means for evaluating a request for access candidate access to the electronic data by the one or more resources, wherein the evaluation of the request includes a second comparison of one or more attributes of the access candidate with one or more access requirements associated with the electronic data;

means for submitting a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, if the second comparison indicates that access to the electronic data by the access candidate is prohibited; and

means for granting the access candidate access to the electronic data using the one or more resources if the resolution authority provides authorization.

17. (Previously Presented) The system as in Claim 16, further comprising means for granting the access candidate access to the electronic data using the one or more resources if the second comparison indicates that access to the electronic data by the access candidate is not prohibited.

18. (Previously Presented) The system as in Claim 16, wherein the access candidate is denied access to the electronic data if the resolution authority denies authorization.

19. (Previously Presented) The system as in Claim 16, wherein the one or more access candidate attributes are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

20. (Previously Presented) The system as in Claim 16, wherein the one or more access requirements associated with the one or more resources relates to at least one of: a valid data access agreement with a potential access candidate; a current location of the potential access candidate; or, a citizenship status of the potential access candidate.

21. (Previously Presented) The system as in Claim 20, wherein the one or more access candidate attributes relates to at least one of: an indication an existence of a data access agreement with the access candidate; a current location of the access candidate; or, a citizenship status of the access candidate.

22. (Previously Presented) The system as in Claim 16, wherein the one or more access requirements associated with the electronic data includes at least one of a current location of the access candidate or a citizenship status of the access candidate.

23. (Previously Presented) A system for providing an access candidate access to secured electronic data, the electronic data being associated with one or more data classes, each data class identifying at least a citizenship requirement and a location requirement for access to data associated with the data class, the system comprising:

storage configured to receive and store the electronic data;

one or more resources configured to process and manipulate the electronic data;

a resource access controller configured to grant access to the one or more resources, in response to a request for access to the one or more resources, based at least

Reply to Office Action of January 4, 2010

in part on a comparison of a citizenship status and a current location of the access candidate and an existence of a data access agreement with a citizenship requirement, wherein the location requirement and the data access agreement requirement are associated with the one or more resources;

one or more data access controllers configured to grant access to a corresponding portion of the electronic data based at least in part on a comparison of the citizenship status and the current location of the access candidate with the citizenship requirement and the location requirement associated with the one or more data classes of the corresponding portion of the electronic data;

one or more resolution authorities, which are configured to modify access requirements associated with the one or more data classes, configured to authorize access to one or more portions of the electronic data in response to a comparison performed by a corresponding data access controller that indicates access is prohibited; and

a data access module configured to:

evaluate a request for access to one or more portions of the electronic data by the one or more resources to identify one or more data access controllers corresponding to the one or more portions of the electronic data; and

forward the request for access to the one or more identified data access controllers for evaluation as to whether to grant the access candidate access to the corresponding one or more portions of the electronic data.

24. (Previously Presented) A method for determining an access candidate access to secured electronic data, the method comprising:

receiving, by a controller associated with the secured electronic data, a request for access to the secured electronic data;

comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the secured electronic data;

submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited; and

Reply to Office Action of January 4, 2010

granting or denying by the controller, in whole or in part, the access candidate access to the secured electronic data based, at least in part, on a determination by the resolution authority regarding whether to authorize access of the access candidate to the secured electronic data, wherein the determination by the resolution authority is based on access candidate information and request related information.

25. (Previously Presented) The method as in Claim 24, further comprising granting the access candidate access to the secured electronic data in response to a comparison that indicates that access by the access candidate is not prohibited.

26. (Previously Presented) The method as in Claim 24, wherein the one or more access requirements associated with the secured electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to the controller via a network.

27. (Previously Presented) The method as in Claim 24, wherein the one or more access requirements associated with the secured electronic data are related to at least one of a citizenship status or a current location of the access candidate.

28. (Previously Presented) The method as in Claim 27, wherein the one or more attributes of the access candidate includes at least one of a citizenship status or a current location of the access candidate.

29. (Previously Presented) A method for determining an access candidate access to secured electronic data, the method comprising:

receiving, by a controller associated with the secured electronic data, a request for access to the secured electronic data;

comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the secured electronic data;

granting the access candidate access to the secured electronic data in response to a comparison that indicates that access by the access candidate is not prohibited; and

submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited; and

granting or denying by the controller, in whole or in part, the access candidate access to the secured electronic data based, at least in part, on a determination by the resolution authority regarding whether to authorize access of the access candidate to the secured electronic data, wherein the determination by the resolution authority is based on access candidate information and request related information.

30. (Previously Presented) In a data security system having a first security level securing one or more resources for manipulating electronic data and a second security level securing access to the electronic data by the one or more resources, a method for determining an access candidate access to the electronic data, the method comprising:

receiving a request for access to the first security level;

granting the access candidate access to the first security level based on a comparison of one or more attributes of the access candidate with one or more access requirements associated with the first security level;

receiving a request for access to the second security level; and

submitting a request for authorization to a resolution authority, which is configured to modify one or more access requirements associated with the second security level, in response to a comparison of one or more attributes of the access candidate with the one or more access requirements associated with the second security level that indicates that access to the second security level by the access candidate is prohibited and to determine whether to authorize the access candidate access to the second security level.

31. (Previously Presented) The method as in Claim 30, further comprising granting the access candidate access to the second security level in response to a comparison of the one or more attributes of the access candidate with the one or more

Reply to Office Action of January 4, 2010

access requirements associated with the second security level that indicates that access to the second security level by the access candidate is not prohibited.

32. (Previously Presented) The method as in Claim 30, further comprising the step of denying the access candidate access to the second security level if the resolution authority denies authorization.

33. (Previously Presented) The method as in Claim 30, wherein the one or more attributes of the access candidate is represented as part of a graphical display associated with the access candidate and accessed for display via a network.

34. (Previously Presented) The method as in Claim 30, wherein the one or more access requirements associated with the first security level relates to at least one of: a valid data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

35. (Previously Presented) The method as in Claim 34, wherein the one or more attributes of the access candidate relates to at least one of: an indication of whether the access candidate has a data access agreement; a current location of the access candidate; or, a citizenship status of the access candidate.

36. (Previously Presented) The method as in Claim 30, wherein the one or more access requirements associated with the second security level relates to at least one of a current location of the access candidate or a citizenship status of the access candidate.

37. (Previously Presented) The method as in Claim 30, wherein at least one of the request for access to the first security level or the request for access to the second security level is submitted by one or more sponsors.

Reply to Office Action of January 4, 2010

38. (Previously Presented) The method as in claim 1, further comprising determining the authorization, by the resolution authority, by granting a waiver of the one or more access requirements associated with the secured electronic data.

39. (Previously Presented) The method as in claim 1, further comprising determining the authorization, by the resolution authority, by modifying the one or more access requirements associated with the secured electronic data.

40. (Previously Presented) The method as in claim 1, further comprising determining the authorization, by the resolution authority, by excluding the electronic data assigned to one or more prohibited data classes from access by the access candidate.

41. (Previously Presented) The method of claim 1, further comprising receiving supplemental evidence verifying the attributes of the access candidate.

42. (Previously Presented) The system of claim 15, wherein the data subsets are separated into the at least one data class based on a data provider of the data.